

*In the Claims*

The status of claims in the case is as follows:

- 1 1. [Currently amended] A method for control and  
2 management of communication traffic, comprising the steps  
3 of:  
  
4 expressing access rules as filters referencing system  
5 kernel data;  
  
6 for outbound processing, determining source application  
7 indicia;  
  
8 for inbound packet processing, executing a look-ahead  
9 function to determine target application indicia; said  
10 look-ahead function being executed within a protocol  
11 stack including an IP layer, a transport layer, a  
12 sockets layer, and an application layer and which, for  
13 said inbound packet, said IP layer provides to said  
14 transport layer said inbound packet, marked as non-  
15 deliverable, and receives back from said transport  
16 layer indicia, provided to said transport layer by said  
17 sockets layer, identifying the application layer  
18 application to which said packet would have been  
19 delivered; and  
  
20 responsive to said source or target application  
21 indicia, executing filter processing; said filter  
22 processing including constructing and evaluating  
23 logical expressions of arbitrary length, and

END920010019US1

2 of 40

S/N 09/919,185

24 selectively using a set of logical operators,  
 25 alternative filter selector fields, and value set.

1 2. [Original] The method of claim 1, further comprising  
 2 the steps of executing said determining and executing steps  
 3 within a kernel filtering function upon encountering a  
 4 filter selector field referencing kernel data not included  
 5 in said packet.

1 3. [Original] The method of claim 1, said filter  
 2 processing including the steps of:

3 determining a task or thread identifier;

4 based on said task or thread identifier, determining a  
 5 process or job identifier; and

6 based on said process or job identifier, determining  
 7 job or process attributes for filter processing.

1 4. [Original] The method of claim 1, said filter  
 2 processing including the steps of:

3 determining a user identifier; and

4 based on said user identifier, determining user  
 5 attributes for filter processing.

1 5. [Original] The method of claim 3, further comprising  
 2 the step of determining from said task identifier a work  
 3 control block containing said process or job identifier.

END920010019US1

3 of 40

S/N 09/919,185

1 6. [Canceled]

2 7. [Canceled]

1 8. [Original] The method of claim 1, further comprising  
2 the steps of:

3 delivering to said filters infrastructure access rules  
4 for defining security context.

1 9. [Original] The method of claim 8, said infrastructure  
2 including logging, auditing, and filter rule load controls.

1 10. [Currently amended] A method for control and  
2 management of aspects of communication traffic within  
3 filtering, comprising the steps of:

4 receiving IP packet data into a TCP/IP protocol stack  
5 executing within a system kernel;

6 for an inbound IP packet, executing a look-ahead  
7 function within a protocol stack including an IP layer,  
8 a transport layer, a sockets layer, and an application  
9 layer and which, for said IP inbound packet, said IP  
10 layer provides to said transport layer said inbound IP  
11 packet, marked as non-deliverable, and receives back  
12 from said transport layer indicia, provided to said  
13 transport layer by said sockets layer, identifying the  
14 application layer application to which said packet  
15 would have been delivered; and

END920010019US1

4 of 40

S/N 09/919,185

16       executing filtering code within said system kernel with  
17       respect to non-IP packet data accessed within said  
18       system kernel outside of said TCP/IP protocol stack;  
19       said filtering code constructing and evaluating logical  
20       expressions of arbitrary length, and selectively using  
21       a set of logical operators, alternative filter selector  
22       fields, and value set.

1       11. [Original] The method of claim 10, said non-IP packet  
2       data including context data regarding said IP packet.

1       12. [Original] The method of claim 10, said non-IP packet  
2       data including data specific to a task generating said non-  
3       IP packet data.

1       13. [Original] The method of claim 10, said non-IP packet  
2       data including data specific to a task that will receive  
3       said IP packet.

1       14. [Original] The method of claim 11, said context data  
2       including packet arrival interface indicia.

1       15. [Canceled]

2       16. [Canceled]

3       17. [Original]

4       18. [Currently amended] A method for centralizing system-  
5       wide communication management and control within filter  
6       rules, comprising the steps of:

7       providing filter statements syntax for accepting  
8       parameters in the form of a selector, each selector

END920010019US1

5 of 40

S/N 09/919,185

9 specifying selector field, operator, and a set of  
10 values; [[and]]  
  
11 for an inbound packet, executing a look-ahead function  
12 within a protocol stack including an IP layer, a  
13 transport layer, a sockets layer, and an application  
14 layer and which, for said inbound packet, said IP layer  
15 provides to said transport layer said inbound packet,  
16 marked as non-deliverable, and receives back from said  
17 transport layer indicia, provided to said transport  
18 layer by said sockets layer, identifying the  
19 application layer application to which said packet  
20 would have been delivered by said sockets layer;

21 said selector referencing data that does not exist in  
22 IP packets;

23 processing said filter statements, including  
24 constructing and evaluating logical expressions of  
25 arbitrary length, and selectively using a set of  
26 logical operators, alternative filter selector fields,  
27 and value set.

1 19. [Original] The method of claim 18, said parameters  
2 selectively including userid, user profile, user class, user  
3 group, user group authority, user special authority, job  
4 name, process name, job group, job class, job priority,  
5 other job or process attributes, and date & time.

1 20. [Original] The method of claim 18, said filters  
2 statements being provided within a user interface to said  
3 system.

END920010019US1

6 of 40

S/N 09/919,185

1 21. [Original] The method of claim 18, further comprising  
2 the steps of:

3 establishing a tunnel between two IP address limiting  
4 traffic to applications bound to ports at each end of  
5 said tunnel;

6 said filtering code accessing filtering attributes  
7 further limiting traffic selectively to job indicia;  
8 and

9 operating said filtering code within a kernel filtering  
10 function upon encountering a filter selector field  
11 referencing kernel data not included in said traffic.

1 22. [Currently amended] A method for traversing a portion  
2 only of a protocol stack to disallow selective IP packet  
3 traffic, comprising the steps of:

4 receiving a packet in the kernel of the operating  
5 system of a first node from an application, said kernel  
6 including a filter processor; said filter processor for  
7 constructing and evaluating logical expressions of  
8 arbitrary length, said logical expressions selectively  
9 including a set of logical operators, alternative  
10 filter selector fields, and value set;

11 for inbound packet processing to a first node from a  
12 second node, executing a look-ahead function in the  
13 system kernel of said first node to determining

END920010019US1

7 of 40

S/N 09/919,185

14 determine a target application; said system kernel  
15 including a protocol stack including an IP layer, a  
16 transport layer, a sockets layer, and an application  
17 layer and which, for said inbound packet, said IP layer  
18 provides to said transport layer said inbound packet,  
19 marked as non-deliverable, and receives back from said  
20 transport layer indicia identifying the application  
21 layer application to which said packet would have been  
22 delivered;

23 for both said inbound packet processing, and for  
24 outbound packet processing from said first node to said  
25 second node, executing within said kernel the steps of

26 processing said packet by determining a task ID;

27 responsive to said task ID, determining a  
28 corresponding work control block;

29 determining a user ID, process or job identifier  
30 from said work control block;

31 from the user ID, process or job identifier  
32 selectively determining attributes for said user  
33 process or job; and

34 passing said attributes to said filter processor  
35 for managing and controlling communication  
36 traffic.

1 23. [Currently amended] A method for expressing access  
2 rules as filters, comprising the steps of:

END920010019US1

8 of 40

S/N 09/919,185

3 providing a filter statements syntax for accepting  
4 parameters in the form of a selector, each selector  
5 specifying selector field, operator, and a set of  
6 values; and

7 said selector referencing data that does not exist in  
8 IP packets for controlling access to an application,

9 for an inbound IP packet, executing a look-ahead  
10 function within a protocol stack including an IP layer,  
11 a transport layer, a sockets layer, and an application  
12 layer and which, for said IP inbound packet, said IP  
13 layer provides to said transport layer said inbound IP  
14 packet, marked as non-deliverable, and receives back  
15 from said transport layer indicia, provided to said  
16 transport layer by said sockets layer, identifying the  
17 application layer application to which said packet  
18 would have been delivered; and

19 processing said filter statements by constructing and  
20 evaluating logical expressions of arbitrary length,  
21 said logical expressions selectively including a set of  
22 logical operators, alternative filter selector fields,  
23 and value set referencing said application layer  
24 application.

1 24. [Currently amended] A method for managing and  
2 controlling communication traffic by centralizing access  
3 rules in filters executing within and referencing data  
4 available in system kernels, comprising the steps for  
5 outbound packet processing from a first node to a second  
6 node of:

END920010019US1

9 of 40

S/N 09/919,185



7 receiving said packet in the kernel of the operating  
8 system of said first node from an application or  
9 process at said first node;

10 processing said packet by determining a task ID;

11 responsive to said task ID, determining a corresponding  
12 work control block;

13 responsive to said work control block, determining a  
14 process or job identifier;

15 responsive to said process or job identifier,  
16 determining job or process attributes; and

17 executing said filters by constructing and evaluating  
18 logical expressions of arbitrary length, said logical  
19 expressions selectively including a set of logical  
20 operators, alternative filter selector fields, and  
21 value set.

1 25. [Currently amended] The method of claim 24, further  
2 comprising the steps for inbound packet processing from said  
3 second node to said first node of:

4 initially operating said kernel at said first node to  
5 determine a target application for said packet at said  
6 first node by executing a look-ahead function within a  
7 protocol stack including an IP layer, a transport  
8 layer, a sockets layer, and an application layer and  
9 which, for said inbound packet, said IP layer provides  
10 to said transport layer said inbound packet, marked as

END920010019US1

10 of 40

S/N 09/919,185

11 non-deliverable, and receives back from said transport  
 12 layer indicia, provided to said transport layer by said  
 13 sockets layer, identifying the application layer  
 14 application to which said packet would have been  
 15 delivered;.

26. [Canceled]

1 27. [Canceled]

2 28. [Canceled]

1 29. [Currently amended] A method for managing and  
 2 controlling communication traffic by centralizing the access  
 3 rules, comprising the steps for outbound packet processing  
 4 from a first node to a second node of:

5 receiving said packet in the kernel of the operating  
 6 system of said first node from an application or  
 7 process at said first node, said kernel including a  
 8 filter processor for constructing and evaluating  
 9 logical expressions of arbitrary length, said logical  
 10 expressions selectively including a set of logical  
 11 operators, alternative filter selector fields, and  
 12 value set;

13 processing said packet by determining a task ID;

14 responsive to said task ID, determining a corresponding  
 15 work control block;

16 determining a user ID control block from said work  
 17 control block;

END920010019US1

11 of 40

S/N 09/919,185

18 from the user ID control block determining attributes  
19 for said user; and

20 passing said attributes to said filter processor for  
21 managing and controlling communication traffic.

1 30. [Currently amended] The method of claim 29, further  
2 comprising the steps for inbound packet processing from said  
3 second node to said first node of:

4 initially operating said kernel at said first node to  
5 determine a target application for said packet at said  
6 first node by executing a look-ahead function within a  
7 protocol stack including an IP layer, a transport  
8 layer, a sockets layer, and an application layer and  
9 which, for said inbound packet, said IP layer provides  
10 to said transport layer said inbound packet, marked as  
11 non-deliverable, and receives back from said transport  
12 layer indicia, provided to said transport layer by said  
13 sockets layer, identifying the application layer  
14 application to which said packet would have been  
15 delivered.

1 31. [Canceled]

2 32. [Canceled]

3 33. [Canceled]

1 34. [Currently amended] A method for control and  
2 management of communication traffic with respect to a system  
3 node, comprising the steps of:

4 receiving at said system node an inbound packet; and

END920010019US1

12 of 40

S/N 09/919,185

5       executing within a protocol stack of the system kernel  
6       of said system node a filtering function identifying  
7       for said inbound packet a filter referencing non-packet  
8       data, and constructing and evaluating logical  
9       expressions of arbitrary length, said logical  
10       expressions selectively including a set of logical  
11       operators, alternative filter selector fields, and  
12       value set; and

13       responsive to said filter, executing a look-ahead  
14       function for identifying a target application for said  
15       inbound packet; said look-ahead function executed  
16       within a protocol stack including an IP layer, a  
17       transport layer, a sockets layer, and an application  
18       layer and which, for said IP inbound packet, said IP  
19       layer provides to said transport layer said inbound  
20       packet, marked as non-deliverable, and receives back  
21       from said transport layer indicia, provided to said  
22       transport layer by said sockets layer, identifying the  
23       application layer application to which said packet  
24       would have been delivered;.

1       35. [Original] The look-ahead function of the method of  
2       claim 34 further comprising the steps of:

3       passing to a transport layer function identified by an  
4       IP header a packet marked non-deliverable for  
5       determining which user-level process or job is to  
6       receive said packet;

7       receiving from said transport layer an application  
8       layer task identifier for said user-level process or

END920010019US1

13 of 40

S/N 09/919,185

9 job; and thereafter

10 passing said packet marked by said task identifier to  
11 said transport layer for delivery to said application  
12 layer task.

1 36. [Currently amended] System for control and management  
2 of communication traffic, comprising:

3 a system kernel including a filter function and stack  
4 data;

5 said filter function including a filter selectively  
6 referencing said stack data for expressing access  
7 rules;

8 said filter function being responsive to receipt of an  
9 outbound packet for determining a source application;

10 said filter function being responsive to receipt of an  
11 inbound packet processing for executing a look-ahead  
12 function within a protocol stack to determine a target  
13 application; said protocol stack including an IP layer,  
14 a transport layer, a sockets layer, and an application  
15 layer and which, for said inbound packet, said IP layer  
16 provides to said transport layer said inbound packet,  
17 marked as non-deliverable, and receives back from said  
18 transport layer indicia, provided to said transport  
19 layer by said sockets layer, identifying the  
20 application layer application to which said packet  
21 would have been delivered; and

END920010019US1

14 of 40

S/N 09/919,185

22 said filter function being responsive to said source or  
23 target application for executing filter processing  
24 including constructing and evaluating logical  
25 expressions of arbitrary length, said logical  
26 expressions selectively including a set of logical  
27 operators, alternative filter selector fields, and  
28 value set.

1 37. [Currently amended] A system for control and  
2 management of aspects of communication traffic within  
3 filtering, comprising:

4 a system kernel;

5 a protocol stack including an IP layer, a transport  
6 layer, a sockets layer, and an application layer for  
7 executing within said system kernel, responsive to an  
8 inbound IP packet, a look-ahead function by which said  
9 IP layer provides to said transport layer said inbound  
10 IP packet, marked as non-deliverable, and receives back  
11 from said transport layer indicia, provided to said  
12 transport layer by said sockets layer, identifying the  
13 application layer application to which said packet  
14 would have been delivered; and

15 filtering code within said system kernel operable with  
16 respect to non-IP packet data accessed within said  
17 system kernel outside of said protocol stack for  
18 controlling and managing said aspects of communication  
19 traffic; said filter code for constructing and  
20 evaluating logical expressions of arbitrary length,  
21 said logical expressions selectively including a set of

END920010019US1

15 of 40

S/N 09/919,185

22 logical operators, alternative filter selector fields,  
23 and value set.

1 38. [Currently amended] A system for centralizing system-  
2 wide communication management and control within filter  
3 rules, comprising:

4 filter statements having a syntax for accepting  
5 parameters in the form of a selector, each selector  
6 specifying selector field, operator, and a set of  
7 values; [[and]]

8 said selector referencing data that does not exist in  
9 IP packets;

10 a look-ahead function within a protocol stack including  
11 an IP layer, a transport layer, a sockets layer, and an  
12 application layer which, for an inbound packet, said IP  
13 layer provides to said transport layer said inbound  
14 packet, marked as non-deliverable, and receives back  
15 from said transport layer indicia, provided to said  
16 transport layer by said sockets layer, for identifying  
17 the application layer application to which said packet  
18 would have been delivered; and

19 a filter processor for constructing and evaluating  
20 filter statements including logical expressions of  
21 arbitrary length, said logical expressions selectively  
22 including a set of logical operators, alternative  
23 filter selector fields, and value set.

1 39. [Currently amended] A system for traversing a portion

END920010019US1

16 of 40

S/N 09/919,185

2       only of a protocol stack to disallow selective IP packet  
3       traffic, comprising:

4           a system kernel;

5           a filter processor executing within said system kernel  
6           for constructing and evaluating logical expressions of  
7           arbitrary length, said logical expressions selectively  
8           including a set of logical operators, alternative  
9           filter selector fields, and value set;

10          said filter processor responsive to an inbound packet  
11          for executing a look-ahead function for determining a  
12          target application; said look-ahead function operating  
13          within a protocol stack including an IP layer, a  
14          transport layer, a sockets layer, and an application  
15          layer and which, for said IP inbound packet, said IP  
16          layer provides to said transport layer said inbound IP  
17          packet, marked as non-deliverable, and receives back  
18          from said transport layer indicia, provided to said  
19          transport layer by said sockets layer, identifying the  
20          application layer application to which said packet  
21          would have been delivered;

22          said filter processor responsive to both inbound and  
23          outbound packets for

24               processing said packet by determining a task ID;

25               responsive to said task ID, determining a  
26               corresponding work control block;

END920010019US1

17 of 40

S/N 09/919,185



27 determining a user ID, process or job identifier  
28 from said work control block;

29 from the user ID, process or job identifier  
30 selectively determining attributes for said user  
31 process or job; and

32 passing said attributes to said filter processor  
33 for managing and controlling communication  
34 traffic.

1 40. [Currently amended] A system for expressing access  
2 rules as filters, comprising:

3 [[a]] filter statements for accepting parameters in the  
4 form of a selector, each selector specifying selector  
5 field, operator, and a set of values; [[and]]

6 said selector referencing data that does not exist in  
7 IP packets for controlling access to an application;

8 a look-ahead function executing within a protocol stack  
9 including an IP layer, a transport layer, a sockets  
10 layer, and an application layer and which, for an  
11 inbound packet, said IP layer provides to said  
12 transport layer said inbound packet, marked as non-  
13 deliverable, and receives back from said transport  
14 layer indicia, provided to said transport layer by said  
15 sockets layer, identifying the application layer  
16 application to which said packet would have been  
17 delivered; and

END920010019US1

18 of 40

S/N 09/919,185

18        a filter processor for constructing and evaluating said  
19        filter statements as logical expressions of arbitrary  
20        length, each said logical expression selectively  
21        including said operator selected from a set of logical  
22        operators, alternative filter selector fields, and  
23        value set.

1        41. [Currently amended] A system for managing and  
2        controlling communication traffic by centralizing access  
3        rules in filters executing within and referencing data  
4        available in system kernels, comprising:

5        a computer readable medium;

6        first code for receiving a packet in the kernel of the  
7        operating system of a first node from an application or  
8        process at said first node; said kernel responsive to  
9        an inbound packet, for executing a look-ahead function  
10       within a protocol stack including an IP layer, a  
11       transport layer, a sockets layer, and an application  
12       layer and which, for said inbound packet, said IP layer  
13       provides to said transport layer said inbound IP  
14       packet, marked as non-deliverable, and receives back  
15       from said transport layer indicia, provided to said  
16       transport layer by said sockets layer, identifying the  
17       application layer application to which said packet  
18       would have been delivered;

19       second code for processing said packet by determining a  
20       task ID;

21       third code responsive to said task ID for determining a

END920010019US1

19 of 40

S/N 09/919,185

22 corresponding work control block;

23 fourth code responsive to said work control block for

24 determining a process or job identifier; [[and]]

25 fifth code responsive to said process or job identifier

26 for determining job or process attributes;

27 sixth code for executing said filters by constructing

28 and evaluating logical expressions of arbitrary length,

29 said logical expressions selectively including a set of

30 logical operators, alternative filter selector fields,

31 and value set; and wherein

32 said first, second, third, fourth, fifth, and sixth

33 code is recorded on said computer readable medium.

1 42. [Canceled]

2 43. [Currently amended] A system for control and

3 management of communication traffic with respect to a system

4 node, comprising:

5 a filtering function executing within a protocol stack

6 of the system kernel of said system node identifying

7 for an inbound packet a filter referencing non-packet

8 data; and

9 a look-ahead function responsive to said filter for

10 identifying a target application for said inbound

11 packet; said look-ahead function functioning within a

12 protocol stack including an IP layer, a transport

END920010019US1

20 of 40

S/N 09/919,185

13 layer, a sockets layer, and an application layer and  
14 which, for said inbound packet, said IP layer provides  
15 to said transport layer said inbound packet, marked as  
16 non-deliverable, and receives back from said transport  
17 layer indicia, provided to said transport layer by said  
18 sockets layer, identifying the application layer  
19 application to which said packet would have been  
20 delivered;; and

21 a filter processor for constructing and evaluating  
22 logical expressions of arbitrary length, said logical  
23 expressions selectively including a set of logical  
24 operators, alternative filter selector fields, and  
25 value set.

44. [Canceled]

1 45. [Currently amended] A computer program product for  
2 control and management of aspects of communication traffic  
3 within filtering, said computer program product comprising:  
  
4 a computer readable medium;  
  
5 first program instructions to receive IP packet data  
6 into a TCP/IP protocol stack executing within a system  
7 kernel including, for processing an inbound IP packet,  
8 a look-ahead function within a protocol stack including  
9 an IP layer, a transport layer, a sockets layer, and an  
10 application layer and which, for said IP inbound  
11 packet, said IP layer provides to said transport layer  
12 said inbound IP packet, marked as non-deliverable, and  
13 receives back from said transport layer indicia,

END920010019US1

21 of 40

S/N 09/919,185

14 provided to said transport layer by said sockets layer,  
15 identifying the application layer application to which  
16 said packet would have been delivered; [[and]]

17 second program instructions to execute filtering code  
18 within said system kernel with respect to non-IP packet  
19 data accessed within said system kernel outside of said  
20 TCP/IP protocol stack by constructing and evaluating  
21 logical expressions of arbitrary length, said logical  
22 expressions selectively including a set of logical  
23 operators, alternative filter selector fields, and  
24 value set; and wherein

25 said first and second program instructions are recorded  
26 on said medium.

1 46. [Currently amended] A [[a]] computer program product  
2 for centralizing system-wide communication management and  
3 control within filter rules, said computer program product  
4 comprising:

5 a computer readable medium;

6 first program instructions to execute filter statements  
7 having a syntax for accepting parameters in the form of  
8 a selector, each selector specifying selector field, a  
9 logical operator selected from a set of a plurality of  
10 logical operators, and a set of values; and

11 second program instructions to cause said selector to  
12 reference data that does not exist in IP packets, said  
13 data including application layer indicia obtained for

14 an incoming packet by a look-ahead function; said look-  
15 ahead function executing within a protocol stack  
16 including an IP layer, a transport layer, a sockets  
17 layer, and an application layer and which, for said IP  
18 inbound packet, said IP layer provides to said  
19 transport layer said inbound IP packet, marked as non-  
20 deliverable, and receives back from said transport  
21 layer indicia, provided to said transport layer by said  
22 sockets layer, identifying the application layer  
23 application to which said packet would have been  
24 delivered; and wherein

25 said first and second program instructions are recorded  
26 on said medium.

1 47. [Currently amended] A [[all] computer program product  
2 for managing and controlling communication traffic by  
3 centralizing access rules in filters executing within and  
4 referencing data available in system kernels, said computer  
5 program product comprising:

6 a computer readable medium;

7 first program instructions to receive said packet in  
8 the kernel of the operating system of said first node  
9 from a process at said first node;

10 second program instructions to process said packet by  
11 determining a task ID;

12 third program instructions, responsive to said task ID,  
13 to determine a corresponding work control block;

END920010019US1

23 of 40

S/N 09/919,185

14 fourth program instructions, responsive to said work  
15 control block, to determine a process or job  
16 identifier; [[and]]

17 fifth program instructions, responsive to said process  
18 or job identifier, to determine job or process  
19 attributes; and

20 sixth program instructions to execute a filter  
21 processor for constructing and evaluating logical  
22 expressions of arbitrary length, said logical  
23 expressions selectively including a set of logical  
24 operators, alternative filter selector fields, and  
25 value set; and wherein

26 said first, second, third, fourth, and fifth fifth, and  
27 sixth program instructions are recorded on said medium.

1 48. [Previously presented] The computer program product of  
2 claim 47, said computer program product further comprising  
3 for inbound packet processing from said second node to said  
4 first node:

5 sixth program instructions to initially operate said  
6 kernel at said first node to determine a target  
7 application for said packet at said first node by  
8 executing a look-ahead function within a protocol stack  
9 including an IP layer, a transport layer, a sockets  
10 layer, and an application layer and which, for said IP  
11 inbound packet, said IP layer provides to said  
12 transport layer said inbound IP packet, marked as non-  
13 deliverable, and receives back from said transport

END920010019US1

24 of 40

S/N 09/919,185

14 layer indicia, provided to said transport layer by said  
15 sockets layer, identifying the application layer  
16 application to which said packet would have been  
17 delivered;; and wherein

18 said sixth program instructions are recorded on said  
19 medium.

1 49. [Currently amended] A computer program product or  
2 ~~computer program element~~ for control and management of  
3 communication traffic, ~~according to the steps~~ comprising:

4 a computer readable medium;

5 first program instructions for expressing access rules  
6 as filters referencing system kernel data;

7 second program instructions, for outbound processing,  
8 for determining a source application;

9 third program instructions, for inbound packet  
10 processing, for executing a look-ahead function to  
11 determine a target application; said look-ahead  
12 function operating within a protocol stack including an  
13 IP layer, a transport layer, a sockets layer, and an  
14 application layer and which, for said IP inbound  
15 packet, said IP layer provides to said transport layer  
16 said inbound IP packet, marked as non-deliverable, and  
17 receives back from said transport layer indicia,  
18 provided to said transport layer by said sockets layer,  
19 identifying the application layer application to which  
20 said packet would have been delivered; [[and]]

END920010019US1

25 of 40

S/N 09/919,185



21 fourth program instructions, selectively responsive to  
 22 said source ~~or target~~ and target application, for  
 23 executing filter processing including constructing and  
 24 evaluating logical expressions of arbitrary length,  
 25 said logical expressions selectively including a set of  
 26 logical operators, alternative filter selector fields,  
 27 and value set;; and wherein

28 said first, second, third, and fourth program  
 29 instructions are recorded on said computer readable  
 30 medium.

1 50. [Currently amended] A computer program product or  
 2 ~~computer program element~~ for control and management of  
 3 aspects of communication traffic within filtering, according  
 4 to ~~steps~~ comprising:

5 a computer readable medium:

6 first program instructions for receiving IP packet data  
 7 into a TCP/IP protocol stack executing within a system  
 8 kernel;

9 second program instructions for executing filtering  
 10 code within said system kernel with respect to non-IP  
 11 packet data accessed within said system kernel outside  
 12 of said TCP/IP protocol stack; said filtering code  
 13 constructing and evaluating logical expressions of  
 14 arbitrary length, said logical expressions selectively  
 15 including a set of logical operators, alternative  
 16 filter selector fields, and value set; and wherein

17 said first and second program instructions are recorded  
18 on said computer readable medium.

1 51. [Currently amended] A ~~computer program product or~~  
2 computer program element for centralizing system-wide  
3 communication management and control within filter rules,  
4 ~~according to method steps comprising:~~

5 a computer readable medium:

6 first program instructions for providing filter  
7 statements syntax for accepting parameters in the form  
8 of a selector, each selector specifying selector field,  
9 a logical operator, and a set of values,

10 second program instructions for executing filtering by  
11 constructing and evaluating logical expressions of  
12 arbitrary length, said logical expressions selectively  
13 including said logical operator selected from a set of  
14 logical operators, at least one said selector field,  
15 and at least one said value; [[and]]

16 said selector referencing data that does not exist in  
17 IP packets including data obtained, for an inbound IP  
18 packet, by executing a look-ahead function within a  
19 protocol stack including an IP layer, a transport  
20 layer, a sockets layer, and an application layer and  
21 which, for said IP inbound packet, said IP layer  
22 provides to said transport layer said inbound IP  
23 packet, marked as non-deliverable, and receives back  
24 from said transport layer indicia, provided to said  
25 transport layer by said sockets layer, identifying the

END920010019US1

27 of 40

S/N 09/919,185

26       application layer application to which said packet  
27       would have been delivered;; and wherein  
  
28       said first and second program instructions are recorded  
29       on said computer readable medium.

1       52. [Currently amended] A computer program product or  
2       ~~computer program element~~ for managing and controlling  
3       communication traffic by centralizing access rules in  
4       filters executing within, and referencing data available in,  
5       system kernels, ~~according to method steps~~ comprising:  
  
6       a computer readable medium:  
  
7       first program instructions for receiving said packet in  
8       the kernel of the operating system of said first node  
9       from an application or process at said first node;  
  
10       second program instructions for processing said packet  
11       by determining a task ID;  
  
12       third program instructions, responsive to said task ID,  
13       for determining a corresponding work control block;  
  
14       fourth program instructions, responsive to said work  
15       control block, for determining a process or job  
16       identifier;  
  
17       fifth program instructions, responsive to said process  
18       or job identifier, for determining job or process  
19       attributes;

END920010019US1

28 of 40

S/N 09/919,185

20 sixth program instructions for executing a filter  
21 processor for constructing and evaluating logical  
22 expressions of arbitrary length, said logical  
23 expressions selectively including a set of logical  
24 operators, alternative filter selector fields, and  
25 value set; and wherein

26 said first, second, third, fourth, fifth, and sixth  
27 program instructions are recorded on said computer  
28 readable medium.

1 53. [Currently amended] The computer program product or  
2 ~~element of claim 52, said method steps~~ further comprising  
3 for inbound packet processing from said second node to said  
4 first node:

5 seventh program instructions initially operating said  
6 kernel at said first node to determine a target  
7 application for said packet at said first node by  
8 executing a look-ahead function within a protocol stack  
9 including an IP layer, a transport layer, a sockets  
10 layer, and an application layer and which, for said IP  
11 inbound packet, said IP layer provides to said  
12 transport layer said inbound IP packet, marked as non-  
13 deliverable, and receives back from said transport  
14 layer indicia, provided to said transport layer by said  
15 sockets layer, identifying the application layer  
16 application to which said packet would have been  
17 delivered;; and wherein

18 said seventh program instructions are recorded on said  
19 computer readable medium.

END920010019US1

29 of 40

S/N 09/919,185